

Acord de prelucrare a datelor cu caracter personal

Versiunea 2026-10-05

Acest acord se încheie între clinica care folosește Perlato (Operatorul) și MPR DESIGN S.R.L. (Persoana împuternicită), în temeiul art. 28 din Regulamentul (UE) 2016/679 (RGPD) și al Legii nr. 190/2018. Partea B preia integral clauzele contractuale standard adoptate de Comisia Europeană prin Decizia de punere în aplicare (UE) 2021/915. Versiunea 2026-10-05.

Partea A — Încheierea și structura acordului

A.1. Părțile. Operatorul este clinica, cabinetul sau entitatea care folosește platforma Perlato („Serviciul”) și stabilește scopurile și mijloacele prelucrării datelor pacienților săi. Persoana împuternicită este MPR DESIGN S.R.L., cu sediul în Str. Constandin Hagi Stoian nr. 166, Târgu-Mureș, jud. Mureș, România, înregistrată la Registrul Comerțului sub nr. J26/559/20.02.2019, CUI 40673723, furnizorul Serviciului. Datele de identificare complete ale părților sunt în Anexa I.

A.2. Forma. Potrivit art. 28 alin. (9) RGPD, acordul se încheie în scris, inclusiv în format electronic. Acordul se încheie în una din următoarele două modalități:

- **online, la înscriere** — prin bifarea căsuței „Am citit și accept Termenii și condițiile și Acordul de prelucrare a datelor” pe pagina de înscriere (pentru planurile Starter și Pro, inclusiv pentru perioada de probă gratuită de 14 zile). Bifarea constituie o semnătură electronică simplă în sensul art. 3 pct. 10 din Regulamentul (UE) nr. 910/2014 (eIDAS) și al Legii nr. 214/2024. Persoana împuternicită păstrează evidența acceptării: data și ora, versiunea acordului, adresa de email, numele clinicii, adresa instanței, adresa IP și browserul folosit;
- **prin semnare** — olograf sau cu semnătură electronică, pe exemplarul tipărit sau în format PDF (de regulă pentru planul Enterprise și pentru clinicile al căror abonament este gestionat direct de Perlato).

A.3. Reprezentarea. Persoana care acceptă sau semnează acordul declară că are dreptul de a reprezenta Operatorul. Dacă nu are acest drept, Operatorul îl poate confirma ulterior în scris; până la confirmare, persoana respectivă răspunde personal în condițiile art. 1309-1311 din Codul civil.

A.4. Momentul încheierii. Acordul produce efecte de la acceptare sau semnare și înainte de introducerea oricăror date ale pacienților în Serviciu. Acordul este accesoriu contractului de prestare a Serviciului (Termenii și condițiile, publicați la perlato.ro/legal/termeni) și durează cât acesta, plus perioada de returnare și ștergere a datelor din clauza C.10.

A.5. Stocare și reproducere. Textul acordului este publicat permanent la perlato.ro/legal/acord-prelucrare-date și poate fi salvat sau tipărit (Legea nr. 365/2002, art. 8). După înscriere, Operatorul primește prin email confirmarea acceptării, cu versiunea și data. Versiunile anterioare se păstrează și se transmit la cerere.

A.6. Structura și ierarhia. Acordul are trei părți și patru anexe: Partea A (încheierea), Partea B (clauzele contractuale standard din Decizia (UE) 2021/915), Partea C (clauze suplimentare permise de clauza 2 litera (b) din Partea B) și Anexele I-IV. În caz de contradicție, prevalează Partea B (clauza 4), apoi Partea C, apoi Termenii și condițiile. Nicio prevedere din Partea C sau din Termeni nu se interpretează în sensul limitării clauzelor din Partea B sau a drepturilor persoanelor vizate.

Partea B — Clauzele contractuale standard (Decizia (UE) 2021/915)

Textul de mai jos reproduce anexa la Decizia de punere în aplicare (UE) 2021/915 a Comisiei din 4 iunie 2021 (JO L 199, 7.6.2021, p. 18). Au fost păstrate opțiunile aplicabile Regulamentului (UE) 2016/679 (operatorul și persoana împuternicită nu sunt instituții ale Uniunii) și s-a ales, la clauza 7.7, opțiunea 2 (autorizație scrisă generală), cu un termen de 30 de zile. Clauza 5 (opțională) nu se aplică.

Secțiunea I

Clauza 1 — Scopul și domeniul de aplicare

(a) Scopul prezentelor clauze contractuale standard („clauzele”) este de a asigura conformitatea cu articolul 28 alineatele (3) și (4) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

(b) Operatorii și persoanele împuternicite de operatori enumerate în anexa I au convenit asupra prezentelor clauze pentru a asigura conformitatea cu articolul 28 alineatele (3) și (4) din Regulamentul (UE) 2016/679.

(c) Prezentele clauze se aplică prelucrării datelor cu caracter personal, astfel cum se specifică în anexa II.

(d) Anexele I-IV fac parte integrantă din clauze.

(e) Prezentele clauze nu aduc atingere obligațiilor care îi revin operatorului în temeiul Regulamentului (UE) 2016/679.

(f) Prezentele clauze nu asigură, prin ele însele, respectarea obligațiilor referitoare la transferurile internaționale în conformitate cu capitolul V din Regulamentul (UE) 2016/679.

Clauza 2 — Caracterul invariabil al clauzelor

(a) Părțile se angajează să nu modifice clauzele, cu excepția cazului în care trebuie să completeze sau să actualizeze informațiile prevăzute în anexe.

(b) Acest lucru nu împiedică părțile să includă clauzele contractuale standard prevăzute în prezentele clauze în cadrul unui contract mai amplu sau să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor sau nu aduc atingere drepturilor sau libertăților fundamentale ale persoanelor vizate.

Clauza 3 — Interpretare

(a) În cazul în care prezentele clauze utilizează termenii definiți în Regulamentul (UE) 2016/679, acești termeni au același sens ca în regulamentul.

(b) Prezentele clauze trebuie citite și interpretate în lumina dispozițiilor Regulamentului (UE) 2016/679.

(c) Prezentele clauze nu trebuie interpretate într-un mod care contravine drepturilor și obligațiilor prevăzute în Regulamentul (UE) 2016/679 sau într-un mod care aduce atingere drepturilor sau libertăților fundamentale ale persoanelor vizate.

Clauza 4 — Ierarhie

În cazul unei contradicții între prezentele clauze și dispozițiile acordurilor conexe dintre părți care există la momentul în care sunt convenite prezentele clauze sau care sunt încheiate ulterior, prevalează prezentele clauze.

Clauza 5 — Clauză privind aderarea unor părți noi

Clauza opțională nu se aplică.

Secțiunea II — Obligațiile părților

Clauza 6 — Descrierea prelucrării (prelucrărilor) datelor

Operațiunile de prelucrare, în special categoriile de date cu caracter personal și scopurile prelucrării datelor cu caracter personal în numele operatorului, sunt specificate în detaliu în anexa II.

Clauza 7 — Obligațiile părților

7.1. Instrucțiuni

(a) Persoana împuternicită de operator prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, cu excepția cazului în care persoanei împuternicite de operator îi revine această obligație în temeiul dreptului Uniunii sau al dreptului intern care i se aplică. În acest caz, persoana împuternicită de operator îl informează pe operator cu privire la respectiva obligație juridică înainte de prelucrare, cu excepția situației în care legislația interzice o astfel de informare din motive importante legate de interesul public. De asemenea, operatorul poate da instrucțiuni ulterioare pe întreaga durată a prelucrării datelor cu caracter personal. Aceste instrucțiuni trebuie să fie întotdeauna documentate.

(b) Persoana împuternicită de operator îl informează imediat pe operator în cazul în care, în opinia sa, instrucțiunile date de operator încalcă Regulamentul (UE) 2016/679 sau dispozițiile aplicabile ale dreptului Uniunii sau ale dreptului intern referitoare la protecția datelor.

7.2. Limitarea scopului

Persoana împuternicită de operator prelucrează datele cu caracter personal numai în scopul (scopurile) specific(e) al(e) prelucrării, astfel cum se prevede în anexa II, cu excepția cazului în care primește instrucțiuni suplimentare din partea operatorului.

7.3. Durata prelucrării datelor cu caracter personal

Prelucrarea de către persoana împuternicită de operator are loc numai pe durata specificată în anexa II.

7.4. Securitatea prelucrării

(a) Persoana împuternicită de operator implementează cel puțin măsurile tehnice și organizatorice specificate în anexa III pentru a asigura securitatea datelor cu caracter personal. Printre aceste măsuri se numără protecția datelor împotriva unei încălcări a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal sau la accesul neautorizat la acestea (încălcarea securității datelor cu caracter personal). La evaluarea nivelului adecvat de securitate, părțile iau în considerare în mod corespunzător stadiul actual al tehnologiei, costurile implementării, natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile la care sunt expuse persoanele vizate.

(b) Persoana împuternicită de operator acordă membrilor personalului său acces la datele cu caracter personal care fac obiectul prelucrării numai în măsura în care acest lucru este strict necesar pentru executarea, gestionarea și monitorizarea contractului. Persoana împuternicită de operator se asigură că persoanele autorizate să prelucreze datele cu caracter personal primesc s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate.

7.5. Date sensibile

Dacă prelucrarea implică date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, date genetice sau date biometrice pentru identificarea unică a unei persoane fizice, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei persoane fizice sau date referitoare la condamnări penale și infracțiuni („date sensibile”), persoana împuternicită de operator aplică restricții specifice și/sau garanții suplimentare.

7.6. Documentație și conformitate

(a) Părțile trebuie să fie în măsură să demonstreze respectarea prezentelor clauze.

(b) Persoana împuternicită de operator răspunde cu promptitudine și în mod adecvat cererilor de informații din partea operatorului cu privire la prelucrarea datelor în conformitate cu prezentele clauze.

(c) Persoana împuternicită de operator pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute în prezentele clauze și care rezultă în mod direct din Regulamentul (UE) 2016/679. De asemenea, la cererea operatorului, persoana împuternicită de operator trebuie să permită efectuarea de audituri ale activităților de prelucrare care fac obiectul prezentelor clauze și să contribuie la aceste audituri, la intervale rezonabile sau dacă există indicii privind nerespectarea prezentelor clauze. În luarea unei decizii privind efectuarea

unei analize sau a unui audit, operatorul poate ține seama de certificările relevante deținute de persoana împuternicită de operator.

(d) Operatorul poate alege să efectueze el însuși auditul sau să mandateze în acest scop un auditor independent. Auditurile pot include, de asemenea, inspecții la sediile sau la instalațiile fizice ale persoanei împuternicite de operator și se efectuează, dacă este cazul, în urma transmiterii unui preaviz rezonabil.

(e) La cerere, părțile pun la dispoziția autorității/autorităților de supraveghere competente informațiile menționate în prezenta clauză, inclusiv rezultatele oricărui audit.

7.7. Recurgerea la subcontractanți

(a) Opțiunea 2 — autorizație scrisă generală: Persoana împuternicită de operator deține autorizația generală din partea operatorului de a recruta subcontractanți care figurează pe o listă convenită. Persoana împuternicită de operator îl informează în mod specific în scris pe operator cu privire la orice modificări preconizate ale listei prin adăugarea sau înlocuirea subcontractanților cu cel puțin 30 de zile înainte, oferindu-i astfel operatorului suficient timp pentru a putea formula obiecții referitoare la aceste modificări înainte de recrutarea subcontractantului (subcontractanților) în cauză. Persoana împuternicită de operator îi furnizează operatorului informațiile de care acesta are nevoie pentru exercitarea dreptului de a formula obiecții.

(b) În cazul în care persoana împuternicită de operator recrutează un subcontractant pentru a desfășura activități de prelucrare specifice (în numele operatorului), trebuie să efectueze recrutarea printr-un contract care să prevadă, pe fond, aceleași obligații în materie de protecție a datelor ca cele care îi revin persoanei împuternicite de operator în conformitate cu prezentele clauze. Persoana împuternicită de operator se asigură că subcontractantul respectă obligațiile care îi revin persoanei împuternicite de operator în temeiul prezentelor clauze și al Regulamentului (UE) 2016/679.

(c) La cererea operatorului, persoana împuternicită de operator îi furnizează operatorului o copie a acestui contract de subcontractare și a oricăror modificări ulterioare. În măsura în care acest lucru este necesar pentru a proteja secretul de afaceri sau alte informații confidențiale, inclusiv date cu caracter personal, persoana împuternicită de operator poate să mascheze textul contractului înainte de a transmite copia.

(d) Persoana împuternicită de operator rămâne pe deplin responsabilă față de operator pentru îndeplinirea obligațiilor subcontractantului în conformitate cu contractul său cu persoana împuternicită de operator. Persoana împuternicită de operator notifică operatorului orice nerespectare de către subcontractant a obligațiilor sale contractuale.

(e) Persoana împuternicită de operator convine cu subcontractantul asupra unei clauze privind terțul beneficiar, conform căreia – în cazul în care persoana împuternicită de operator a dispărut în fapt, și-a încetat existența de drept sau a devenit insolubil – operatorul are dreptul de a rezilia contractul cu subcontractantul și de a-i da subcontractantului instrucțiuni să șteargă sau să returneze datele cu caracter personal.

7.8. Transferuri internaționale

(a) Orice transfer de date către o țară terță sau o organizație internațională realizat de persoana împuternicită de operator are loc pe baza instrucțiunilor documentate din partea operatorului sau pentru a îndeplini o cerință specifică în temeiul dreptului Uniunii sau al dreptului intern care i se aplică persoanei împuternicite de operator și se desfășoară în conformitate cu capitolul V din Regulamentul (UE) 2016/679.

(b) Operatorul este de acord că, în cazul în care persoana împuternicită de operator recrutează un subcontractant în conformitate cu clauza 7.7 pentru a desfășura activități de prelucrare specifice (în numele operatorului) și respectivele activități de prelucrare implică un transfer de date cu caracter personal în sensul capitolului V din Regulamentul (UE) 2016/679, persoana împuternicită de operator și subcontractantul pot asigura respectarea dispozițiilor prevăzute în capitolul V din Regulamentul (UE) 2016/679 prin recurgerea la clauzele contractuale standard adoptate de Comisie în conformitate cu articolul 46 alineatul (2) din Regulamentul (UE) 2016/679, cu condiția îndeplinirii condițiilor privind recurgerea la respectivele clauze contractuale standard.

Clauza 8 — Asistența acordată operatorului

(a) Persoana împuternicită de operator notifică imediat operatorului orice cerere primită din partea unei persoane vizate. Persoana împuternicită de operator răspunde cererii respective doar dacă a fost autorizată să facă acest lucru de către operator.

(b) Persoana împuternicită de operator trebuie să îi acorde asistență operatorului în îndeplinirea obligațiilor acestuia de a răspunde cererilor formulate de persoanele vizate pentru a-și exercita drepturile, ținând seama de natura prelucrării. În îndeplinirea obligațiilor care îi revin în conformitate cu literele (a) și (b), persoana împuternicită de operator respectă instrucțiunile operatorului.

(c) În plus față de obligația persoanei împuternicite de operator de a-i acorda asistență operatorului în temeiul clauzei 8 litera (b), persoana împuternicită de operator îi acordă asistență acestuia și în ceea ce privește asigurarea respectării următoarelor obligații, ținând seama de natura prelucrării datelor și de informațiile aflate la dispoziția persoanei împuternicite de operator:

- 1 obligația de a efectua o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal (o „evaluare a impactului asupra protecției datelor”), în cazul în care un tip de prelucrare este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice;
- 2 obligația de a consulta autoritatea/autoritățile de supraveghere competentă/competente înainte de prelucrare, în cazul în care o evaluare a impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului;
- 3 obligația de a se asigura că datele cu caracter personal sunt exacte și actualizate, prin înștiințarea operatorului fără întârziere în cazul în care persoana împuternicită de operator a luat cunoștință de faptul că datele cu caracter personal prelucrate sunt inexacte sau nu mai sunt de actualitate;
- 4 obligațiile prevăzute la articolul 32 din Regulamentul (UE) 2016/679.

(d) Părțile stabilesc în anexa III măsurile tehnice și organizatorice adecvate prin intermediul cărora persoana împuternicită de operator are obligația de a-i acorda asistență operatorului în aplicarea prezentei clauze, precum și domeniul de aplicare și amplitudinea asistenței necesare.

Clauza 9 — Notificarea încălcării securității datelor cu caracter personal

În cazul în care are loc o încălcare a securității datelor cu caracter personal, persoana împuternicită de operator cooperează cu operatorul și îi acordă asistență necesară pentru ca acesta să își respecte obligațiile care îi revin în temeiul articolelor 33 și 34 din Regulamentul (UE) 2016/679, dacă este cazul, ținând seama de natura prelucrării și de informațiile aflate la dispoziția persoanei împuternicite de operator.

9.1. Încălcarea securității datelor privind date prelucrate de operator

În cazul în care are loc o încălcare a securității datelor cu caracter personal privind date prelucrate de operator, persoana împuternicită de operator îi acordă asistență operatorului:

(a) în notificarea încălcării securității datelor cu caracter personal către autoritatea/autoritățile de supraveghere competentă/competente, fără întârzieri nejustificate, după ce operatorul a luat cunoștință de aceasta, dacă este cazul (cu excepția cazului în care încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice);

(b) în obținerea următoarelor informații care, în temeiul articolului 33 alineatul (3) din Regulamentul (UE) 2016/679, trebuie să fie menționate în notificarea adresată operatorului și să includă cel puțin:

- 1 natura datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate în cauză, precum și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;
- 2 consecințele probabile ale încălcării securității datelor cu caracter personal;

- 3 măsurile luate sau propuse spre a fi luate de operator pentru a remedia încălcarea securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Atunci când și în măsura în care nu este posibil să se furnizeze toate aceste informații în același timp, notificarea inițială trebuie să conțină informațiile disponibile la momentul respectiv, informațiile suplimentare urmând să fie puse la dispoziție ulterior, fără întârzieri nejustificate, pe măsură ce devin disponibile.

(c) în respectarea, în temeiul articolului 34 din Regulamentul (UE) 2016/679, a obligației de a informa, fără întârzieri nejustificate, persoana vizată cu privire la încălcarea securității datelor cu caracter personal, atunci când încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.

9.2. Încălcarea securității datelor privind date prelucrate de persoana împuternicită de operator

În cazul în care are loc o încălcare a securității datelor cu caracter personal privind date prelucrate de persoana împuternicită de operator, aceasta din urmă, după ce a luat cunoștință de respectiva încălcare, transmite, fără întârzieri nejustificate, o notificare operatorului. Această notificare trebuie să conțină cel puțin:

(a) o descriere a caracterului încălcării securității datelor (inclusiv, acolo unde este posibil, categoriile de persoane vizate în cauză, precum și numărul aproximativ de persoane vizate și de înregistrări de date în cauză);

(b) coordonatele unui punct de contact de unde se pot obține mai multe informații privind încălcarea securității datelor cu caracter personal;

(c) consecințele probabile ale încălcării securității datelor și măsurile luate sau propuse spre a fi luate pentru a remedia încălcarea securității datelor, inclusiv pentru atenuarea eventualelor sale efecte negative.

Atunci când și în măsura în care nu este posibil să se furnizeze toate aceste informații în același timp, notificarea inițială trebuie să conțină informațiile disponibile la momentul respectiv, informațiile suplimentare urmând să fie puse la dispoziție ulterior, fără întârzieri nejustificate, pe măsură ce devin disponibile.

Părțile stabilesc în anexa III toate celelalte elemente pe care trebuie să le furnizeze persoana împuternicită de operator atunci când îi acordă asistență operatorului pentru ca acesta să își respecte obligațiile care îi revin în temeiul articolelor 33 și 34 din Regulamentul (UE) 2016/679.

Secțiunea III — Dispoziții finale

Clauza 10 — Nerespectarea clauzelor și rezilierea

(a) Fără a aduce atingere dispozițiilor Regulamentului (UE) 2016/679, în cazul în care persoana împuternicită de operator nu respectă obligațiile care îi revin în temeiul prezentelor clauze, operatorul poate da instrucțiuni persoanei împuternicite de operator să suspende prelucrarea datelor cu caracter personal până când aceasta din urmă se conformează prezentelor clauze sau până când se reziliază contractul. Persoana împuternicită de operator îl informează cu promptitudine pe operator în cazul în care nu este în măsură să respecte prezentele clauze, indiferent de motiv.

(b) Operatorul are dreptul de a rezilia contractul în măsura în care acesta are ca obiect prelucrarea datelor cu caracter personal în conformitate cu prezentele clauze, dacă:

- 1 prelucrarea datelor cu caracter personal de către persoana împuternicită de operator a fost suspendată de operator în temeiul literei (a) și dacă respectarea prezentelor clauze nu este restabilă într-un termen rezonabil și, în orice caz, în termen de o lună de la suspendare;
- 2 persoana împuternicită de operator a încălcat în mod substanțial sau repetat prezentele clauze sau obligațiile care îi revin în temeiul Regulamentului (UE) 2016/679;

3 persoana împuternicită de operator nu respectă o decizie cu caracter obligatoriu pronunțată de o instanță competentă sau emisă de autoritatea/de autoritățile de supraveghere competentă/competente în legătură cu obligațiile care îi revin în temeiul prezentelor clauze sau în temeiul Regulamentului (UE) 2016/679.

(c) Persoana împuternicită de operator are dreptul de a rezilia contractul în măsura în care acesta are ca obiect prelucrarea datelor cu caracter personal în temeiul prezentelor clauze, în cazul în care, după ce l-a informat pe operator că instrucțiunile sale încalcă obligațiile juridice aplicabile în conformitate cu clauza 7.1 litera (b), operatorul insistă asupra respectării instrucțiunilor.

(d) În urma rezilierii contractului, la alegerea operatorului, persoana împuternicită de operator șterge toate datele cu caracter personal prelucrate în numele operatorului și îi prezintă operatorului dovada faptului că a întreprins această acțiune sau îi returnează operatorului toate datele cu caracter personal și șterge copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede obligația stocării datelor cu caracter personal. Până la ștergerea sau returnarea datelor, operatorul trebuie să continue să asigure respectarea acestor clauze.

Partea C — Clauze suplimentare

Clauzele din această parte completează Partea B, în condițiile clauzei 2 litera (b). Ele nu restrâng nicio obligație din Partea B.

C.1. Instrucțiunile documentate

Constituie instrucțiuni documentate ale Operatorului, în sensul clauzei 7.1: (i) prezentul acord și Termenii și condițiile; (ii) configurarea Serviciului făcută de utilizatorii Operatorului (modulele și integrările activate, setările clinicii, rolurile și conturile create); (iii) acțiunile utilizatorilor Operatorului în Serviciu (de exemplu, trimiterea unui mesaj, emiterea unei facturi, exportul sau ștergerea unei fișe); (iv) cererile scrise trimise de reprezentanții Operatorului la adresa contact@perlato.ro. Operatorul răspunde pentru conturile pe care le creează și pentru drepturile acordate utilizatorilor săi.

C.2. Garanții pentru datele privind sănătatea (completează clauza 7.5)

Pentru datele sensibile din Anexa II, Persoana împuternicită aplică următoarele restricții și garanții:

- **nicio utilizare în scopuri proprii** — datele pacienților nu sunt folosite pentru scopurile proprii ale Persoanei împuternicite: nu sunt vândute, nu sunt folosite pentru publicitate, profilare sau statistici proprii și nu sunt folosite pentru antrenarea, testarea sau îmbunătățirea unor modele de inteligență artificială. O asemenea utilizare ar face din Persoana împuternicită operator, în sensul art. 28 alin. (10) RGPD;
- **acces restrâns** — personalul Persoanei împuternicite accesează datele dintr-o instanță numai pentru operarea tehnică a Serviciului (backup, restaurare, actualizare, remedierea unei erori) sau la cererea Operatorului, iar accesul se limitează la ce este strict necesar;
- **izolare** — datele fiecărui Operator sunt păstrate într-o instanță separată, cu bază de date proprie, fără tabele comune cu alte clinici;
- **funcțiile de inteligență artificială** — funcțiile care trimit text către un furnizor extern de AI (Anexa IV) se folosesc numai la acțiunea unui utilizator al Operatorului și produc sugestii pe care le validează un om; ele nu iau decizii cu efecte juridice asupra pacienților și nu creează profiluri. Prelucrarea datelor privind sănătatea în scopul unui proces decizional automatizat sau al creării de profiluri este permisă doar în condițiile art. 3 alin. (1) din Legea nr. 190/2018. Operatorul poate opri oricând furnizorul extern din Setări (furnizorul „local”, fără transfer);
- **secretul profesional** — Persoana împuternicită și personalul său păstrează confidențialitatea informațiilor despre pacienți și după încetarea acordului, în spiritul regulilor de confidențialitate din Legea nr. 46/2003 a drepturilor pacientului.

C.3. Codul numeric personal

Dacă Operatorul prelucrează CNP-ul pacienților (de exemplu, pe rețete, unde este cerut de normele Ministerului Sănătății, sau pe facturi), Persoana împuternicită aplică măsurile din Anexa III (acces pe roluri, criptare în tranzit, jurnalizare, instruire periodică a personalului), corespunzătoare garanțiilor din art. 4 din Legea nr. 190/2018. Temeiul și necesitatea colectării CNP-ului sunt stabilite de Operator.

C.4. Încălcarea securității datelor (completează clauza 9.2)

Persoana împuternicită notifică Operatorul fără întârzieri nejustificate și, în orice caz, în cel mult 48 de ore de la momentul în care a luat cunoștință de o încălcare a securității datelor privind datele Operatorului, astfel încât Operatorul să poată notifica ANSPDCP în termenul de 72 de ore prevăzut de art. 33 RGPD. Notificarea se trimite prin email la adresa de contact a contului de administrator și, dacă este posibil, prin telefon. Punctul de contact al Persoanei împuternicite este contact@perlato.ro. Persoana împuternicită documentează fiecare încălcare (fapte, efecte, măsuri) și pune documentația la dispoziția Operatorului.

C.5. Cererile persoanelor vizate (completează clauza 8)

Serviciul pune la dispoziția Operatorului instrumente cu care acesta răspunde direct cererilor pacienților: consultarea și corectarea fișei, exportul fișei medicale în format PDF, exportul datelor în format CSV, ștergerea definitivă a unui pacient cu toate datele asociate. Dacă Persoana împuternicită primește direct o cerere de la o persoană vizată, o transmite Operatorului imediat și, în orice caz, în cel mult 2 zile lucrătoare, fără să răspundă pe fond, cu excepția cazului în care Operatorul o autorizează.

C.6. Auditul (completează clauza 7.6)

Informațiile necesare pentru demonstrarea conformității (Anexa III, lista subîmputerniciților, răspunsuri la chestionare de securitate) se transmit în cel mult 15 zile lucrătoare de la cerere. O inspecție la fața locului se anunță cu un preaviz de cel puțin 15 zile lucrătoare, se desfășoară în timpul programului de lucru, fără acces la datele altor clienți și cu respectarea confidențialității, de regulă cel mult o dată pe an; limita anuală nu se aplică dacă există indicii de nerespectare a clauzelor, după o încălcare a securității datelor sau la cererea unei autorități de supraveghere. Fiecare parte își suportă propriile costuri, cu excepția cazului în care auditul constată o încălcare a acordului de către Persoana împuternicită.

C.7. Subîmputerniciții (completează clauza 7.7)

Lista convenită a subîmputerniciților este Anexa IV, publicată și actualizată la perlato.ro/legal/subprocesatori. Informarea prealabilă de 30 de zile se face prin email, la adresa de contact a contului. Dacă Operatorul obiectează motivat și părțile nu găsesc o soluție în termenul de preaviz, Operatorul poate rezilia abonamentul fără penalități, cu export complet al datelor. La cerere, Persoana împuternicită comunică și identitatea subîmputerniciților subcontractanților săi, în măsura în care o cunoaște (Avizul CEPD nr. 22/2024).

C.8. Transferuri în afara Spațiului Economic European (completează clauza 7.8)

Datele instanțelor sunt găzduite în Uniunea Europeană. Un transfer în afara SEE are loc numai prin subîmputerniciții din Anexa IV marcați corespunzător și numai când Operatorul activează funcția respectivă (de exemplu, mesageria WhatsApp, recepția AI sau sincronizarea cu Google Calendar) — activarea constituie instrucțiunea documentată a Operatorului. Transferul se întemeiază pe decizia de adecvare privind Cadrul UE-SUA pentru protecția datelor (Decizia de punere în aplicare (UE) 2023/1795 a Comisiei din 10 iulie 2023), atunci când importatorul este certificat, sau, în lipsa acesteia, pe clauzele contractuale standard din Decizia de punere în aplicare (UE) 2021/914, însoțite de o evaluare a impactului transferului.

C.9. Asistență la evaluarea impactului

Preluarea pe scară largă a datelor privind sănătatea se află pe lista operațiunilor pentru care evaluarea impactului este obligatorie (Decizia ANSPDCP nr. 174/2018). Dacă Operatorul trebuie să efectueze o evaluare a impactului, Persoana împuternicită îi pune la dispoziție, gratuit, descrierea

Serviciului, a fluxurilor de date, a măsurilor din Anexa III și a subîmputerniciților.

C.10. Returnarea și ștergerea datelor la încetare (completează clauza 10 litera (d))

- **exportul în timpul contractului** — Operatorul își poate exporta oricând datele din Serviciu (fișe în PDF, liste în CSV, copia de siguranță completă a bazei de date), fără costuri suplimentare;
- **perioada de recuperare** — la încetarea abonamentului, instanța este oprită, dar datele se păstrează neschimbate cel puțin 30 de zile, în care Operatorul poate cere, gratuit, exportul complet al datelor într-un format structurat, utilizat în mod curent și care poate fi citit automat, inclusiv pentru mutarea la alt furnizor (Regulamentul (UE) 2023/2854, „Regulamentul privind datele”, art. 25 și art. 29). Perioada se prelungește la cerere, cât timp există o cerere de export nesoluționată;
- **ștergerea** — după perioada de recuperare, Persoana împuternicită șterge datele din instanță în cel mult 30 de zile și confirmă ștergerea în scris, la cerere. Copiile din backup-urile criptate se elimină prin rotația automată a acestora, în cel mult 6 luni de la încetare; până atunci rămân criptate, inaccesibile în operare și sunt folosite numai pentru o restaurare cerută de Operator;
- **arhivarea medicală este obligația Operatorului** — documentele medicale se păstrează 5 ani de la data ultimului contact cu pacientul, dacă legea nu prevede un alt termen (art. 35 din Codul deontologic al medicului stomatolog, 2021), iar alte categorii de documente au termenele lor legale (de exemplu, documentele financiar-contabile). Persoana împuternicită nu este arhivatorul Operatorului: de aceea returnarea datelor precedă ștergerea, iar Operatorul răspunde de păstrarea exportului pe durata termenelor legale.

C.11. Responsabilul cu protecția datelor

Fiecare parte evaluează obligația de a desemna un responsabil cu protecția datelor, potrivit art. 37-39 RGPD și art. 10 din Legea nr. 190/2018, și comunică celeilalte părți datele de contact ale acestuia, dacă l-a desemnat. Până la o astfel de comunicare, punctul de contact pentru protecția datelor al Persoanei împuternicite este contact@perlato.ro.

C.12. Răspundere

Răspunderea față de persoanele vizate este cea prevăzută de art. 82 RGPD și nu poate fi limitată prin contract. În raporturile dintre părți se aplică limitarea răspunderii din Termenii și condițiile, cu excepția prejudiciilor cauzate cu intenție sau din culpă gravă (art. 1355 din Codul civil) și a amenzilor aplicate unei părți pentru încălcările proprii, pe care fiecare parte le suportă.

C.13. Modificări

Anexele se actualizează în condițiile clauzei 2 litera (a); lista subîmputerniciților, în condițiile clauzei 7.7 și ale clauzei C.7. Orice altă modificare a acordului se publică la adresa din clauza A.5 și se comunică prin email cu cel puțin 30 de zile înainte de a produce efecte. Dacă Operatorul nu este de acord, poate rezilia abonamentul înainte de data intrării în vigoare, fără penalități, cu export complet al datelor; modificările impuse de lege sau de o autoritate pot produce efecte mai devreme.

C.14. Legea aplicabilă și litigii

Acordul este guvernat de legea română și de dreptul Uniunii. Autoritatea de supraveghere competentă este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP). Litigiile se soluționează pe cale amiabilă, iar în caz de nereușită, de instanțele competente de la sediul Persoanei împuternicite.

Anexa I — Lista părților

Operator: clinica, cabinetul sau entitatea care acceptă acordul la înscriere sau îl semnează. La acceptarea online, Operatorul este identificat prin datele introduse la înscriere (numele clinicii, adresa de email a contului, adresa instanței <clinica>.perlato.ro) și prin datele de facturare ale abonamentului; persoana de contact este titularul contului de administrator (proprietar), iar data aderării este data acceptării, înregistrată de Persoana împuternicită. La semnarea pe hârtie sau PDF, se completează câmpurile de mai jos.

Câmp	Operator
Denumire	
Sediu / adresă	
CUI și nr. de înregistrare	
Reprezentant legal (nume, funcție)	
Persoană de contact pentru protecția datelor (nume, email, telefon)	
Responsabil cu protecția datelor (dacă a fost desemnat)	
Semnătura și data aderării	

Persoana împuternicită:

Câmp	Persoana împuternicită
Denumire	MPR DESIGN S.R.L.
Sediu	Str. Constandin Hagi Stoian nr. 166, Târgu-Mureș, jud. Mureș, România
CUI și nr. de înregistrare	40673723, J26/559/20.02.2019
Reprezentant legal	administratorul societății
Punct de contact pentru protecția datelor	contact@perlato.ro
Semnătura și data aderării	prin publicarea și aplicarea acordului (acceptare online) sau semnătura reprezentantului legal (semnare)

Anexa II — Descrierea prelucrării

Element	Descriere
Categoriile de persoane vizate	Pacienții Operatorului și reprezentanții lor legali; persoanele care solicită o programare sau o ofertă (potențiali pacienți); membrii personalului Operatorului care folosesc Serviciul (medici, asistenți, recepție, administrare); persoanele de contact ale furnizorilor și laboratoarelor Operatorului.
Categoriile de date cu caracter personal	Date de identificare și contact (nume, prenume, telefon, email, adresă, data nașterii, CNP sau document de identitate, după caz); date despre programări și istoricul vizitelor; comunicări cu pacientul (mesaje WhatsApp, SMS, email); planuri de tratament, oferte și acorduri semnate electronic (cu data, adresa IP și dispozitivul semnării); date de facturare și încasare; pentru personal: nume, email, rol, jurnale de acces și pontaj.

Element	Descriere
Date sensibile	Date privind sănătatea: anamneză și alergii, fișe de consultație, diagnostic, dentogramă, proceduri efectuate, rețete, consimțământul informat, imagini medicale (radiografii, fotografii intraorale) și documente încărcate. Restricții și garanții: clauza C.2 și Anexa III (izolare pe instanță, acces pe roluri, jurnalizare, fără utilizare în scopuri proprii sau pentru antrenarea AI, transferuri numai la activarea funcției de către Operator).
Natura prelucrării	Găzduire, stocare, organizare, consultare, modificare, afișare, transmitere către canalele configurate de Operator (mesagerie, facturare, casă de marcat, calendar), backup și restaurare, export, ștergere.
Scopurile prelucrării în numele Operatorului	Furnizarea Serviciului de gestiune a clinicii: programări și calendar, fișa pacientului și documentația medicală, planuri de tratament, comunicarea cu pacienții (remindere, confirmări, cereri de recenzie, campanii activate de Operator), facturare și încasări, rapoarte pentru Operator, suport tehnic, securitatea și continuitatea Serviciului.
Durata prelucrării	Pe durata abonamentului, apoi perioada de recuperare și ștergere din clauza C.10.
Prelucrarea de către subîmpunerniciți	Obiectul, natura și durata pentru fiecare subîmpunernicit sunt descrise în Anexa IV; durata nu depășește durata prezentului acord, cu excepția rotației backup-urilor criptate descrise la clauza C.10.

Anexa III — Măsurile tehnice și organizatorice

Măsurile de mai jos descriu Serviciul la data versiunii acordului și se revizuiesc periodic.

Domeniu	Măsurile
Izolarea datelor	Fiecare clinică are o instanță separată: container propriu și bază de date proprie, pe adresa <clnica>.perlato.ro. Nu există o bază de date comună a pacienților mai multor clinici.
Criptare în tranzit	HTTPS (TLS) pe toate conexiunile, cu certificate Let's Encrypt reînnoite automat; antete de securitate (HSTS, politica de conținut, interzicerea încadrării paginilor în alte site-uri).
Criptare la repaus	Backup-urile trimise în afara serverului sunt criptate înainte de transfer, cu o cheie păstrată numai de Persoana împuternicită.
Identificarea și autorizarea utilizatorilor	Conturi individuale pentru fiecare membru al personalului; parole stocate numai sub formă de hash PBKDF2-SHA256 cu 600.000 de iterații; sesiuni cu token stocat hash-uit (SHA-256) și cu expirare; primul cont de administrator al unei clinici noi se creează numai cu un cod unic trimis Operatorului; limitarea numărului de încercări de autentificare.
Controlul accesului pe roluri	Rolurile proprietar, manager, medic și recepție; datele financiare, salarizarea, setările clinicii, exporturile, importul de date și gestionarea utilizatorilor sunt rezervate rolurilor de conducere; un medic vede numai indicatorii proprii.
Jurnalizare și responsabilitate	Jurnal de audit pentru operațiunile sensibile (ștergeri, facturi, exporturi, modificări de roluri, corecturi de pontaj); istoricul complet al modificărilor fișei de consultație; acordurile semnate electronic păstrează textul semnat, amprenta SHA-256, data, IP-ul și dispozitivul.
Disponibilitate și reziliență	Backup automat zilnic al bazei de date (copie consistentă) pe volumul instanței și copie off-site criptată, cu retenție de 7 zile, 4 săptămâni și 6 luni; procedură de restaurare testată; monitorizarea disponibilității Serviciului, cu alertă.

Domeniu	Măsuri
Securitatea aplicației	Limitarea cererilor pe adresă IP; protecție împotriva cererilor către adrese interne (anti-SSRF) la integrări; secretele integrărilor (WhatsApp, SMS, facturare) sunt mascate în interfață; licență semnată criptografic (Ed25519); documentația tehnică internă a API-ului este oprită în producție; actualizări de securitate aplicate periodic.
Securitate fizică	Servere în centre de date ale furnizorului de găzduire din Uniunea Europeană (Germania), cu acces fizic controlat de acesta (Anexa IV).
Minimizarea datelor	Integrările externe (API, webhook-uri) nu transmit observațiile clinice; mesajele automate conțin numai datele necesare (nume, oră, adresă); funcțiile AI primesc numai textul analizat.
Ștergere și portabilitate	Ștergere definitivă a unui pacient cu toate datele asociate, din aplicație; export PDF al fișei, export CSV, copie completă a bazei de date; procedura din clauza C.10 la încetare.
Măsuri organizatorice	Acces administrativ la servere numai pentru personalul autorizat al Persoanei împuternicite, prin conexiuni autentificate și criptate; obligație de confidențialitate scrisă pentru oricine are acces; instruire periodică privind protecția datelor; procedură de răspuns la incidente cu notificarea Operatorului în termenul din clauza C.4.
Asistența acordată Operatorului	Instrumentele din clauza C.5 pentru cererile pacienților; informațiile din clauza C.9 pentru evaluarea impactului; notificarea încălcărilor cu conținutul din clauza 9.2 și termenul din clauza C.4; răspuns la cereri de informații în termenul din clauza C.6.

Anexa IV — Lista subîmputerniciților

Operatorul autorizează, în condițiile clauzei 7.7 (opțiunea 2), subîmputerniciții din lista publicată la perlato.ro/legal/subprocesatori, care face parte integrantă din acest acord. La data versiunii acordului, lista este:

Subîmputernicit	Prelucrarea	Locația / transferul
Hetzner Online GmbH (Germania)	Găzduirea instanțelor și a bazelor de date, backup zilnic. Toate datele instanței. Pe durata acordului.	Uniunea Europeană (Germania). Fără transfer.
Backblaze, Inc.	Păstrarea copiei off-site a backup-urilor, criptate înainte de transfer (cheia rămâne la Perlato). Pe durata acordului și rotația din clauza C.10.	Regiune UE. Fără transfer de date în clar.
Brevo (Sendinblue SAS, Franța)	Emailuri trimise de Serviciu (activare, notificări, planuri de tratament trimise pacienților, dacă clinica nu folosește propriul server de email). Adresa de email, conținutul mesajului.	Uniunea Europeană.
SMSO Technologies S.R.L. (România)	Trimiterea SMS-urilor, numai pentru clinicile care activează SMS-ul. Număr de telefon, textul mesajului.	România.
Meta Platforms Ireland Ltd. (WhatsApp Business Platform)	Trimiterea și primirea mesajelor WhatsApp, numai pentru clinicile care activează WhatsApp. Număr de telefon, conținutul mesajelor.	UE/SEE; posibil transfer către SUA (clauza C.8).

Subîmputernicit	Prelucrarea	Locația / transferul
OpenAI, L.L.C. (SUA)	Funcțiile de recepție AI, numai la acțiunea unui utilizator al clinicii. Textul analizat; datele nu sunt folosite la antrenarea modelelor (API).	SUA — transfer în condițiile clauzei C.8.
Google Ireland Ltd. (Google Calendar)	Sincronizarea programărilor, numai pentru clinicile care conectează contul. Titlul, ora și durata programării.	UE/global — transfer în condițiile clauzei C.8.
Stripe Payments Europe Ltd. (Irlanda)	Plata abonamentului Operatorului. Date de facturare ale clinicii (nu date ale pacienților).	UE; posibil transfer către SUA (clauza C.8).
Cloudflare, Inc.	DNS pentru domeniul perlato.ro. Nu prelucrează date ale pacienților: traficul aplicației nu trece prin Cloudflare.	—

Programul de facturare (SmartBill, Oblio sau FGO), programul casei de marcat, aplicația SMS Gateway folosită pe telefonul clinicii (inclusiv serverul ei în modul cloud) și furnizorul de email propriu al clinicii, atunci când sunt conectate de Operator, sunt aleși și contractați direct de Operator și primesc datele la instrucțiunea acestuia; ei nu sunt subîmputerniciți ai Persoanei împuternicite.

Semnături (numai la încheierea prin semnare — clauza A.2)

Încheiat în două exemplare originale sau în format electronic, câte unul pentru fiecare parte.

OPERATOR	PERSOANA ÎMPUTERNICITĂ MPR DESIGN S.R.L.
Denumire:	Nume și funcție reprezentant:
Nume și funcție reprezentant:	Semnătura:
Semnătura:	Data:
Data:	